CODING METHOD AND SYSTEM WITH ENHANCED SECURITY

CROSS REFERENCE TO RELATED APPLICATION

Reference is hereby made to the following co-pending U.S. application dealing with related subject matter and assigned to the assignee of the present invention: "A System for the Secure and Rapid Acquisition of Composite Code Signals" by Earl M. Kartchner et al, U.S. Ser. No. 65,040, filed Aug. 19, 1970.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to spread spectrum communication systems and, more particularly, is concerned with a method and system for nonlinearizing spread spectrum codes for enhanced system security while still maintaining rapid acquisition thereof.

2. Description of the Prior Art

The present invention constitutes an improvement upon the system described and illustrated in the above cross-referenced U.S. patent application.

The system of the referenced application utilizes, by way of example, a plurality of linear PN component codes, $C_1, C_2, \ldots C_n$, which are all relatively prime with respect to each other, have an approximately equal number of binary ONES and ZEROES, and, with respect to linear MAJ and MOD composites thereof, possess the following correlation properties:

(1) $C_1, C_2, \ldots$ and C_n each correlates with MAJ ($C_1, C_2, \ldots C_n$) fifty percent of the time.

(2) $C_1, C_2, \ldots$ and C_n each does not correlate with MOD ($C_1, C_2, \ldots C_n$).

(3) MAJ ($C_1, C_2, \ldots C_n$) correlates with MOD ($C_1, C_2, \ldots C_n$) fifty percent of the time.

MAJ ($C_1, C_2, \ldots C_n$) equals a Boolean majority vote of $C_1, C_2, \ldots$ and C_n.

MOD ($C_1, C_2, \ldots C_n$) equals a modulo-2 addition of $C_1, C_2, \ldots$ and C_n.

The chronological sequence of events carried out for achieving rapid code acquisition by the prior art system may be summarized as follows:

(1) Linear component codes, $C_1, C_2, \ldots C_n$, are generated.

(2) $C_1, C_2, \ldots C_n$ are combined in accordance with the Boolean majority voting rule to form a linear acquisition composite code, MAJ ($C_1, C_2, \ldots C_n$).

(3) The acquisition composite code is transmitted.

(4) Upon receipt of the acquisition composite code, linear reference component codes, $R_1, R_2, \ldots R_n$ which correlate respectively with $C_1, C_2, \ldots C_n$, are generated.

(5) First, R_1 is correlated with MAJ ($C_1, C_2, \ldots C_n$); then R_2 is correlated with MAJ ($C_1, C_2, \ldots C_n$; finally, R_n is correlated with MAJ ($C_1, C_2, \ldots C_n$).

For the transmission and receipt of data, the following chronological sequence of events is carried out by the prior art system:

(1) Linear reference component codes, $R_1, R_2, \ldots R_n$, are combined in accordance with the modulo-2 addition rule to form a linear reference composite code, MOD ($R_1, R_2, \ldots R_n$).

(2) MOD ($R_1, R_2, \ldots R_n$) is then correlated with acquisition composite code MAJ ($C_1, C_2, \ldots C_n$).

(3) Linear composite codes, $C_1, C_2, \ldots C_n$, are then combined in accordance with the modulo-2 addition rule to form a linear data-carrying composite code, MOD ($C_1, C_2, \ldots C_n$).

(4) The data-carrying composite code is then transmitted, instead of the acquisition composite code.

(5) At the receiver, MOD ($R_1, R_2, \ldots R_n$) now correlates with MOD ($C_1, C_2, \ldots C_n$).

The above-described sequence of events implies that the total number of code bits required to be searched for acquisition of the transmitted composite code is equal to the sum of the individual lengths of the component codes which form the composite code, rather than the product of their lengths. Consequently, it is readily appreciated that acquisition under the prior art system is rapid, thereby leaving little time for an intelligent jammer to analyze the linear composite code MAJ ($C_1, C_2, \ldots C_n$), which is transmitted for acquisition, in order to determine component codes, $C_1, C_2, \ldots C_n$.

Also, the jammer must have knowledge of all of the component codes and their phase relationship with respect to each other in order to jam MOD ($C_1, C_2, \ldots C_n$) which is used for data transmission, since none of the component codes correlate with MOD ($C_1, C_2, \ldots C_n$).

However, under field conditions where the jammer is capable of intercepting the transmission of MOD ($C_1, C_2, \ldots C_n$), the latter is vulnerable to discovery through analysis by the jammer since it is a linear sequence. By using a computer to perform well known mathmatical calculations at high speed, the polynomial equation which mathematically represents the intercepted linear composite code can be determined and a replica thereof constructed. Therefore, while the overall sequence of events carried out by the prior art system increases the difficulty of code analysis by an enemy, it does not preclude such analysis under certain field conditions in view of the fact that the component codes and the composites thereof being utilized by the prior art system are all linear sequences.

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, certain important modifications are made to the prior art system which result in an improved system being essentially invulnerable to enemy analysis. The above-summarized correlation properties of the prior art system and its concomitant rapid acquisition capability are maintained in the improved system of the present invention, while the likelihood of successful analysis by an enemy of the codes produced by the improved system is made infinitesimally small.

The same basic component codes, $C_1, C_2, \ldots C_n$ and $R_1, R_2, \ldots R_n$, as utilized in the prior art system, are utilized by the improved system during the initial steps in the production of composite codes and in the later acquisition thereof, respectively. However, means in the form of an encrypter running in the decrypt mode is incorporated by the improved system in a manner which insures that the MAJ and MOD composite codes produced are both nonlinear, have the appearance of being of infinite length, and, consequently, are essentially nonanalyzable. Furthermore, the component code, C_n, is not transmitted as a correlatable component of the MAJ acquisition composite code; therefore, the sequence of component codes, $C_1, C_2, \ldots C_n$, which drives the encrypter cannot be determined by analysis of the MAJ composite code even if component codes,